Consolidated Technology Services • WA

Service Inquiry
RPC Over HTTPS

December 17, 2012

Service Description

Outlook Anywhere, formerly known as RPC over HTTP, synchronizes mail between Exchange and Outlook clients using a persistent data file (.ost) on the remote machine who use MS Outlook 2007, 2010 or 2013. This data file is encrypted and secured with the userid/password of the Exchange user. SSL is used to securely transmit the data from client to server.

The “Outlook Anywhere” function in Exchange 2010 should be split into two parts:

- State owned machines
- Non-state owned

RPC over HTTPS is in-use for clients on the internal network to provide Exchange integration and includes security for data in-transit.

State Owned Devices

State owned devices can take advantage of the “outlook anywhere” function while mitigating many of the security risks:

- Global security policy can be enforced on state owned devices machines
- Existing agency acceptable use policies govern the use of state equipment by employees
- Authentication leverages existing Enterprise Active Directory integration
- Remote Access can be limited to a particular AD group(s) to restrict access
- Existing security applications and controls deployed on state owned devices can be leveraged to provide a secure environment

The use of “outlook anywhere” does not allow for access to the Vault without the use of VPN

Non-State Owned

Enabling Outlook Anywhere on non-state owned devices presents a significant risk to state data and cannot enforce the same security mitigations used on state owned devices:

Security concerns include:

- State AD security policy cannot be distributed to non-domain joined personal devices creating a higher risk environment
- Anti-virus on personal devices is not managed by state IT staff increasing the risk of virus and malware infiltration
- Existing agency acceptable use and e-discovery policies for state devices may not be acceptable nor enforceable on personal devices or could be limited in scope
- Personal mail could be imported into state systems and state mail could be exported into personal mail clients increasing risk and complicating e-discovery
- Outlook Anywhere encrypts mail data using AD credentials but a lack of disk encryption could result in higher data loss risk
- Personal devices may not have security products and settings enabled such as firewalls and password protected access
- Devices owned by employees are often shared which would increase risks to state data
- If a device is shared and a user closes Outlook, but does not lock their computer it is possible for an unauthorized user to restart Outlook, and access the user's email.

The primary benefit would be the increased mobility and access for state exchange users without limitation of devices.

Recommendation

Based on the potential risk to the state, the recommendation is to not allow "Outlook Anywhere" for non-state owned devices.